2010 Data Protection Seminar

TMA Privacy Office

Developing a Legal Foundation

HEALTH AFFAIRS

TRICARE
Management Activity

Developing a Legal Foundation

Purpose

Provide an overview of the laws that will be discussed during the Data Protection Seminar

Objectives

- Upon completion of this presentation, you should be able to:
  - State the purpose of each law, who it applies to, and what it protects
  - Recognize that laws create standards and mandate compliance
  - Identify how different laws relate to one another

Developing a Legal Foundation

The Privacy Act

- Purpose: Balance the government's need to maintain information about individuals with the rights of individuals
  - Restricts disclosure of personally identifiable records
  - Grants individuals increased rights of access to records
- To whom it applies: Federal Government agencies
- What it protects: Information about individuals held in systems of records
- Implementation standard: DoD 5400.11-R, "DoD Privacy Program"

Developing a Legal Foundation

HIPAA

- Purpose: The Health Insurance Portability and Accountability Act (HIPAA) improves the efficiency and effectiveness of the health care system by standardizing the electronic exchange of administrative and financial data
- To whom it applies:
  - Covered Entities (CEs), including health plans, health care clearinghouses, and health care providers who transmit health information electronically in connection with certain transactions set forth in the regulations
  - Business Associates (BAs), as directed by the Health Information Technology for Economic and Clinical Health (HITECH) Act

Developing a Legal Foundation

HIPAA (continued)

- What it protects: Protected health information (PHI)
- Implementation standards:
  - DoD 6025.18-R, “DoD Health Information Privacy Regulation”
  - DoD 8580.02-R, “DoD Health Information Security Regulation”

Developing a Legal Foundation

The HITECH Act

- Purpose: The HITECH Act seeks to improve American health care delivery and patient care through health information technology and expanded privacy and security provisions
- To whom it applies: CEs, as described previously, BAs, vendors of personal health records, and certain non-HIPAA CEs
- What it protects: PHI
- Implementation standards: Currently under review

Developing a Legal Foundation

FOIA

- Purpose: The Freedom of Information Act (FOIA) informs the public through responsible disclosure of information while appropriately protecting all interests and acts as a key tool for open government
- To whom it applies: Federal Government agencies
- What it protects: Individuals' right to know what the government is doing
- Implementation standards:
  - DoD Directive 5400.7, "DoD Freedom of Information Act (FOIA) Program"
  - DoD 5400.7-R, "DoD Freedom of Information Act Program"

Developing a Legal Foundation

E-Government Act

- Purpose: Improve Internet-based technology to make it easier for citizens and businesses to interact with the government
- To whom it applies: Federal Government agencies
- What it protects: Personally identifiable information (PII) that agencies collect, maintain, or disseminate when developing or securing information technology
- Implementation standards:
  - DoD Federal Information Security Management Act (FISMA) Guidance 2009
  - DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance"

Developing a Legal Foundation

FISMA

- Purpose: The FISMA provides a comprehensive framework for ensuring effectiveness of information security controls over information resources that support federal operations and assets
- To whom it applies:
  - Federal Government agencies' information systems
  - Information systems operated by contractors on behalf of federal agencies
- What it protects: Federal information systems and related resources

Developing a Legal Foundation

FISMA (continued)

- Implementation standards:
  - DoD FISMA Guidance 2009
  - DoD Directive 8500.1, “Information Assurance”
  - DoD Instruction 8500.2, “Information Assurance (IA) Implementation”
  - DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP)”

Developing a Legal Foundation

Paperwork Reduction Act

- Purpose: Reduce the total amount of paperwork handled by the Federal Government and general public, and maximize utility of information
- To whom it applies:
  - Federal Government agencies
  - Businesses, organizations, and individuals who do business with the Federal Government
- What it protects: Information created, collected, maintained, used, disseminated, or disposed
- Implementation standard: DoD 8910.1-M, "DoD Procedures for Management of Information Requirements"

Developing a Legal Foundation

Records Management

- Purpose: National Archives and Records Administration (NARA) regulations support the creation, maintenance and use, and disposition of records to document federal policies, operations, and transactions appropriately and economically
- To whom it applies: Federal Government agencies and businesses, organizations, and individuals who do business with the government
- What it protects: Information created, maintained, disseminated, or received by an agency related to the public business of that agency

Developing a Legal Foundation

Records Management (continued)

- Implementation standards:
  - Administrative Instruction 15, “Office of the Secretary of Defense Records Management Administrative Procedures and Records Disposition Schedules, Volumes I & II
  - DoD Directive 5015.2, “DoD Records Management Program”

Developing a Legal Foundation

Integrating Different Laws

- Different laws with different purposes often govern at the same time
- Compliance with all applicable laws is required

Developing a Legal Foundation

Summary

- You should now be able to:
  - State the purpose of each law, who it applies to, and what it protects
  - Recognize that laws create standards and mandate compliance
  - Identify how different laws relate to one another

Developing a Legal Foundation

Definitions

- PII: Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual

Source: DoD 5400.11-R, "DoD Privacy Program", May 14, 2007

Definitions (continued)

- PHI: Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records held by TMA in its role as an employer

Source: DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 24, 2003

Developing a Legal Foundation

Resources

- The Privacy Act of 1974, as amended (5 U.S.C § 552a)
- Administrative Instruction 15, "Office of the Secretary of Defense Records Management Administrative Procedures and Records Disposition Schedules", Volumes I & II, August 11, 1994
- Paperwork Reduction Act, Public Law 104-13, May 22, 1995
- Freedom of Information Act (FOIA), July 4, 1996
- Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, August 21, 1996
- DoD Manual 8910.1-M, "DoD Procedures for Management of Information Requirements", June 30, 1998

Developing a Legal Foundation

Resources (continued)

- DoD Regulation 5400.7-R, “DoD Freedom of Information Act Program”, September 1998
- DoD Directive 5015.2, “DoD Records Management Program”, March 6, 2000
- OMB Circular No. A-130, Revised, Transmittal No. 4, November 30, 2000
- DoD Directive 8500.1, “Information Assurance”, October 24, 2002
- E-Government Act, Public Law 107-347, of 2002

Developing a Legal Foundation

Resources (continued)

- Federal Information Security Management Act (FISMA) of 2002
- DoD Regulation 6025.18-R, “DoD Health Information Privacy Regulation”, January 24, 2003
- DoD Instruction 8500.2, “Information Assurance (IA) Implementation”, February 6, 2003
- DoD Directive 5400.7, “DoD Freedom of Information (FOIA) Act Program”, October 28, 2005
- DoD CIO Memorandum, “DoD Privacy Impact Assessment (PIA) Guidance”, October 28, 2005

Developing a Legal Foundation

Resources (continued)

- DoD Regulation 5400.11-R, “DoD Privacy Program”, May 14, 2007
- DoD Regulation 8580.02-R, “DoD Health Information Security Regulation”, July 12, 2007
- DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP)”, November 28, 2007
- DoD Directive 8000.01, “Management of the Department of Defense Information Enterprise”, February 10, 2009

Developing a Legal Foundation

Resources (continued)

- DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance", February 12, 2009
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, February 17, 2009
- DoD FISMA Guidance, May 2009
- To subscribe to the TMA Privacy Office E-News, go to: http://www.tricare.mil/tma/privacy/mailinglist.aspx
- E-mail Privacymail@tma.osd.mil for subject matter questions